МАТЕМАТИЧЕСКИЕ ОСНОВЫ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

УДК 004.94 DOI 10.17223/20710410/61/5

МОДЕЛЬ И МЕТРИКИ ОСВЕДОМЛЕННОСТИ В КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ. ЧАСТЬ 1. ПОТЕНЦИАЛЬНАЯ ОСВЕДОМЛЕННОСТЬ

Н. А. Гайдамакин

Уральский федеральный университет имени первого Президента России Б. Н. Ельцина, г. Екатеринбург, Россия

E-mail: n.a.gaidamakin@urfu.ru

В рамках субъектно-объектной формализации компьютерных систем введены понятия потенциальной и фактической осведомлённости пользователей в конфиденциальной информации. Потенциальная осведомлённость рассматривается как величина, определяющаяся имеющимися у пользователя правами доступа к объектам, содержащим конфиденциальную информацию, и объёмом конфиденциальной информации соответствующих объектов. Объём конфиденциальной информации объекта предложено определять на основе количества слов, содержащихся в тексте объекта, и величины информативности объекта, которая устанавливается внешним фактором, например автором и/или выделенным пользователем (аналитиком). Для основных моделей управления доступом (дискреционной, мандатной, тематико-иерархической и ролевой) представлены аналитические соотношения, определяющие в количественной шкале диапазона $[0, 1]$ величину потенциальной осведомлённости пользователей в конфиденциальной информации, содержащейся (обрабатывающейся) в компьютерной системе. Доказано удовлетворение соответствующих величин требованиям метрики.

Ключевые слова: *конфиденциальная информация, осведомлённость, потенциальная осведомлённость, модель осведомлённости, метрики осведомлённости, управление доступом, права доступа, субъекты доступа, объекты доступа.*

THE MODEL AND METRICS OF AWARENESS IN CONFIDENTIAL INFORMATION. PART 1. POTENTIAL AWARENESS

N. A. Gaydamakin

Ural Federal University named after the first President of Russia B. N. Yeltsin, Ekaterinburg, Russia

As part of the subject-object formalization of computer systems, the concepts of potential and actual user awareness of confidential information are introduced. Potential awareness is considered as a value determined by the user's access rights to objects containing confidential information and the volume of confidential information of the corresponding objects. The volume of confidential information of the object is proposed to be determined on the basis of the number of words contained in the text of the

object and the amount of information content of the object, which is determined by an external factor, for example, the author and/or a dedicated user (analyst). For the main access control models (discretionary, mandatory, thematic-hierarchical and role-based), analytical relations are presented that determine, on a quantitative scale of the range $[0, 1]$, the amount of potential awareness of users in confidential information contained (processed) in a computer system. The satisfaction of the corresponding values to the metric requirements is proved.

Keywords: *confidential information, awareness, potential awareness, awareness model, awareness metrics, access control, access rights, access subject, access objects.*

Введение

Анализ осведомлённости в конфиденциальной информации является важной составляющей мониторинга процессов обеспечения информационной безопасности.

В толковом словаре Ушакова [1] «*осведомлённость*» определяется как *знание, наличие сведений о чем-либо*. В практической и нормативной сфере употребляется смежный, во многих случаях синонимичный, термин «*владение информацией*». Иначе говоря, быть осведомлённым означает владеть определённой информацией, т. е. знать соответствующие сведения, сообщения, данные, составляющие (выражающие) информацию.

В качестве субъекта владения рассматривается человек, являющийся в контексте компьютерной сферы пользователем, осуществляющим доступ к информации, точнее, к объектам, содержащим конфиденциальную информацию.

Модели управления доступом пользователей к информации в компьютерных системах [2, 3] регламентируют правила санкционирования доступов в соответствии с правами, задаваемыми явно (дискреционная модель — DAC, Discretionary Access Control) или посредством соотношения меток безопасности (мандатная модель — MAC, Mandatory Access Control). В рамках имеющихся прав пользователи осуществляют доступы к объектам, в результате которых формируется их осведомлённость в конфиденциальной информации, содержащейся (обрабатывающейся) в компьютерной системе. Соответственно можно выделить «потенциальную» и «фактическую» осведомлённость.

Потенциальная осведомлённость (Potential Awareness) пользователя определяется имеющимися у него правами доступа, реализуя которые, пользователь может стать осведомлённым в конфиденциальной информации.

Фактическая осведомлённость (Actual Awareness) пользователя является результатом осуществления доступов к конфиденциальной информации.

Рассмотрение формализованной и процедурно-аналитической стороны потенциальной осведомлённости является предметом данной работы.

1. Исходные положения

Будем использовать распространённую парадигму в сфере компьютерной безопасности, в рамках которой компьютерная система рассматривается как совокупность субъектов и объектов доступа. Под *субъектами*, именуемыми активными сущностями, понимаются выполняющиеся по командам пользователей компьютерные программы. Под *объектами*, именуемыми пассивными сущностями, понимаются элементарные информационные структуры (файлы, таблицы баз данных, их строки, поля, записи) или составные (каталоги, базы данных), к которым пользователями осуществляется доступ на чтение или запись (изменение).

В рамках субъектно-объектного подхода сделаем несколько исходных предположений и определений.

Положение 1. Компьютерная система представляется множеством объектов доступа $o \in O$ и множеством субъектов доступа $s \in S$, которые управляются пользователями $u \in U$.

В дальнейшем в процессах анализа доступов к объектам будем отождествлять понятие субъекта и пользователя, оговаривая особенности такого допущения в необходимых случаях.

Положение 2. В компьютерной системе действует дискретное время, в каждый момент t_k которого пользователи $u \in U$ посредством субъектов $s \in S$ осуществляют доступы к объектам $o \in O$.

Определение 1. Под *доступом* будем понимать имеющий временны́е рамки процесс воздействия субъекта $s \in S$ на объект $o \in O$, в результате которого формируется поток информации — однонаправленный, т. е. от объекта к субъекту или от субъекта (через субъект) к объекту, либо двунаправленный, т. е. одновременно от субъекта к объекту и от объекта к субъекту.

Однонаправленный поток от объекта к субъекту реализуется в рамках доступа вида «Чтение» (Read), от субъекта к объекту — вида «запись» (Write). Двунаправленный поток реализуется в рамках доступов вида «Чтение» и «Запись», одновременно осуществляемых субъектом к соответствующему объекту. Далее в контексте анализа осведомлённости ограничимся рассмотрением только доступов вида «Чтение» к объектам, содержащим текстовую информацию.

Существуют различные подходы к понятию *информационного потока*. В частности, в «детерминистской» трактовке информационный поток рассматривается как процесс изменения слова, характеризующего (описывающего, составляющего) объект-приёмник, в который поступает информация в виде слова, характеризующего объект-источник информационного потока [4]. В теоретико-информационном смысле объект доступа рассматривается как слово некоторого языка в определённом алфавите. В рамках отмеченных ограничений (рассмотрение только доступов вида «Read» к объектам, содержащим текстовую информацию) соответствующим языком будем считать естественный язык письменной речи. Под «словом» понимается в том числе и совокупность слов, характеризующих, выражающих информацию или часть информации объекта. В теоретико-вероятностной трактовке информационный поток рассматривается как процесс изменения неопределённости состояния объекта (изменения множества его возможных состояний) [5].

Отметим, что при «детерминистском» подходе в случае чтения объекта изменяется слово, характеризующее состояние субъекта, точнее, домена, выделенного субъекту [4], т. е. областей (буферов) оперативной памяти компьютерного устройства, в которых размещаются исполняемый код и данные соответствующего вычислительного процесса и визуальное отображение которых непосредственно воспринимается пользователем. Иначе говоря, в упрощённой трактовке объектом-приёмником при чтении объекта можно считать области оперативной видеопамяти, выделенной вычислительному процессу субъекта.

Определение 2. Под *объёмом* (*количеством*) $V(o_n, t_k)$ *конфиденциальной информации* объекта o_n понимается величина, пропорциональная количеству слов $Q(o_n, t_k)$, содержащихся в момент времени t_k в тексте объекта o_n:

$$V(o_n, t_k) = Q(o_n, t_k)\theta(o_n, t_k),$$

где $\theta(o_n, t_k)$ — изменяющийся в диапазоне $[0, 1]$ коэффициент информативности объекта o_n в момент времени t_k (1 — максимальная информативность).

Введение коэффициента информативности $\theta(o_n, t_k)$ обусловлено тем, что языком письменной речи одну и ту же информацию можно выразить по-разному, с разной ясностью, чёткостью, полнотой, «понятностью» и, следовательно, с различным словесным объёмом. Очевидно, что информативность является скорее качественным понятием, но будем считать, что существует вещественнозначная функция, выражающая данное свойство объектов в числовом диапазоне $[0, 1]$.

Фундаментальным в сфере компьютерной безопасности является понятие конфиденциальности информации. В специальной литературе и нормативных документах приводятся различные определения понятия конфиденциальности информации [6–8], отталкиваясь от которых дадим следующее определение.

Определение 3. Под *конфиденциальностью* информации будем понимать такое свойство информации, устанавливаемое федеральным законом либо обладателем информации, когда может быть причинён ущерб гражданам, организациям, обществу, государству либо обладателю информации при свободном обороте таковой информации (свободном доступе к ней и соответственно осведомлённости в ней неопределённого круга лиц), при условии того, что информация известна только уполномоченным лицам и обладателем информации принимаются и реализуются меры по ограничению доступа к этой информации неуполномоченных лиц.

Таким образом, конфиденциальность является свойством определённой информации. Иначе говоря, не все объекты доступа содержат конфиденциальную информацию или не вся информация объекта является конфиденциальной.

Конфиденциальность как свойство информации является качественным понятием и в дискреционной модели управления доступом рассматривается как дихотомическая характеристика (информация «конфиденциальна/неконфиденциальна»), в мандатной модели — как характеристика в порядково-вербальной шкале (как правило, в трёх градациях — «высокая конфиденциальность», «средняя», «низкая»). В практических приложениях могут использоваться расширенные системы классификации конфиденциальности информации с большим количеством градаций с квалиметрическими характеристиками каждого уровня [9, Приложение А].

Из определения 3 следует, что конфиденциальность информации может изменяться с течением времени.

Положение 3. Существует вещественнозначная функция $f_{\text{conf}}(o_n, t_k)$, которая каждому объекту компьютерной системы $o_n \in O$ в каждый момент времени t_k ставит в соответствие некоторую величину (значение) конфиденциальности $\mathcal{K} = f_{\text{conf}}(o_n, t_k)$.

Функцию конфиденциальности $f_{\text{conf}}(o_n, t_m)$ в системах дискреционного и мандатного управления доступом можно рассматривать как кусочно-постоянную функцию, значения которой в интересах нормирования устанавливаются в диапазоне $[0, 1]$ (рис. 1 и 2). В общем случае вид и параметры функции $f_{\text{conf}}(o_n, t_k)$ определяются особенностями предметной области и обладателем информации (собственником компьютерной системы).

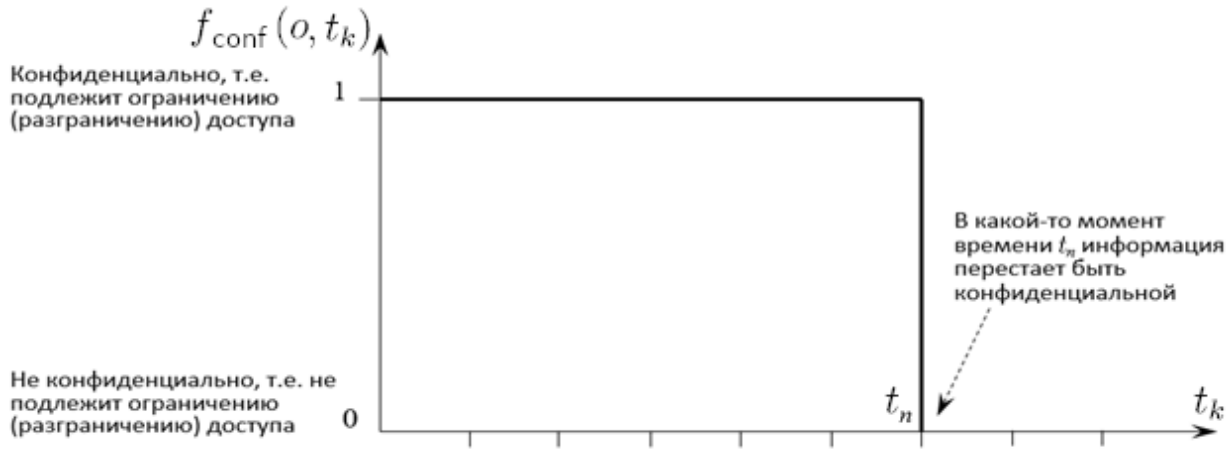

Рис. 1. Пример функции конфиденциальности объектов $f_{\text{conf}}(o, t_k)$ при дискреционном управлении доступом

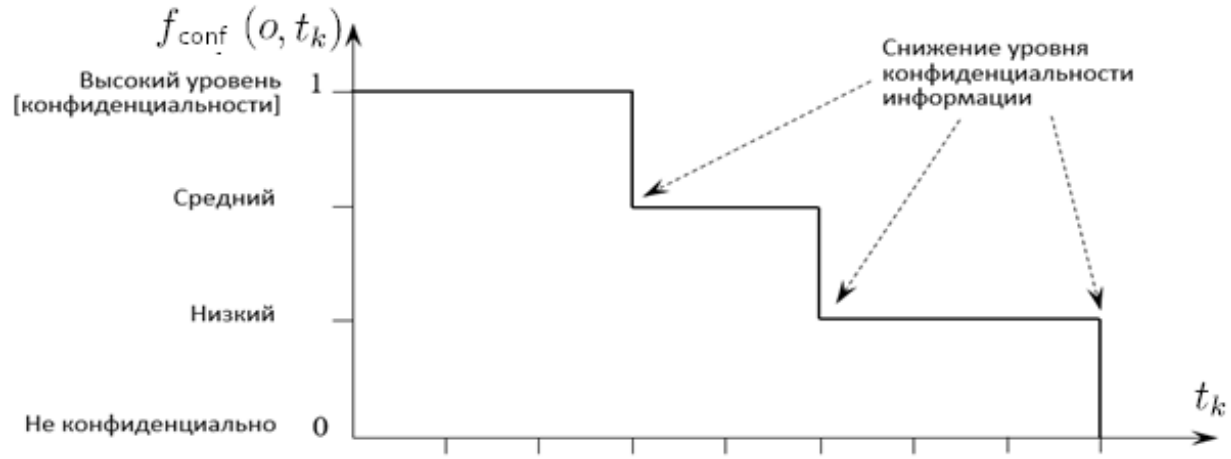

Рис. 2. Пример функции конфиденциальности объектов $f_{\text{conf}}(o, t_k)$ при мандатном управлении доступом

2. Потенциальная осведомлённость пользователей в конфиденциальной информации в системах дискреционного управления доступом

В дискреционной модели управления доступом (DAC) права пользователей на доступ к объектам устанавливаются явно в виде троек «пользователь — разрешённая операция доступа — объект» и фиксируются в тех или иных информационных структурах (ACL, Access Control List — списки управления доступом к файлам в операционных системах; системные таблицы прав доступа баз данных в СУБД).

Математическим образом соответствующих структур, в частности совокупности ACL файлов в операционных системах является матрица доступа $\mathbf{A}$, строки которой соответствуют пользователям $u_l \in U$, столбцы — объектам доступа $o_n \in O$, в ячейках

записываются идентификаторы разрешённых процедур доступа, например:

$$\mathbf{A} = \begin{array}{c} \\ u_1 \\ u_2 \\ \dots \\ u_L \end{array} \begin{array}{c} \begin{array}{cccc} o_1 & o_2 & \dots & o_N \end{array} \\ \begin{pmatrix} \text{Read} & - & \dots & - \\ - & \text{Read, Write} & \dots & \text{Read} \\ \dots & \dots & \dots & \dots \\ \text{Write} & - & \dots & \text{Read, Write} \end{pmatrix} \end{array}. \tag{1}$$

Каждый ACL рассматривается как столбец матрицы доступа, из которого удалены все пустые ячейки. Поскольку в процессе анализа осведомлённости мы ограничились только доступами «Чтение» (Read), то элементы матрицы доступа a_{ln} будем представлять двоичными числами:

$$a_{ln} = \begin{cases} 1, & \text{если Read} \in (\mathbf{A})_{ln}; \\ 0, & \text{если Read} \notin (\mathbf{A})_{ln}. \end{cases}$$

В такой кодировке матрица доступа (1) выглядит следующим образом:

$$\mathbf{A} = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 1 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 \end{pmatrix}.$$

Как в теоретических моделях управления доступом, так и при их практической реализации в компьютерных системах права доступа пользователей к объектам могут изменяться. Отсюда с учётом положения 2 матрица доступа является динамическим объектом, т. е. её структура (размеры) и значения элементов могут быть различными в разные моменты времени. Данное обстоятельство будем отображать временной зависимостью матрицы доступа и её элементов — $\mathbf{A}(t_k), a_{ln}(t_k)$.

Сделаем следующее очевидное предположение.

Положение 4. *Потенциальная осведомлённость* (*Potential Awareness*) пользователя в конфиденциальной информации тем больше, чем больше у него прав доступа к объектам компьютерной системы и чем больше конфиденциальной информации имеется в соответствующих объектах.

Очевидно, ситуацию, в которой пользователь имеет права доступа на чтение ко всем объектам компьютерной системы, можно охарактеризовать как максимальную (100 %) потенциальную осведомлённость.

Тогда, основываясь на положении 4, потенциальную осведомлённость $\mathcal{A}_{\text{DAC\_Pot}}(u_l, t_k)$ пользователя u_l в конфиденциальной информации компьютерной системы в момент времени t_k при дискреционном управлении доступом можно определять как

$$\mathcal{A}_{\text{DAC\_Pot}}(u_l, t_k) = \frac{1}{V(O, t_k)} \sum_{n=1}^{N_{t_k}} a_{ln}(t_k) V(o_n, t_k),$$

где $V(O, t_k)$ — объём конфиденциальной информации, содержащейся во всех объектах компьютерной системы в момент времени t_k:

$$V(O, t_k) = \sum_{n=1}^{N_{t_k}} V(o_n, t_k); \tag{2}$$

N_{t_k} — количество объектов с конфиденциальной информацией в момент времени t_k. Нетрудно видеть, что если пользователь имеет право доступа на чтение всех объектов компьютерной системы, то его потенциальная осведомлённость $\mathcal{A}_{\text{DAC\_Pot}}(u_l, t_k) = 1$, т. е. 100 %. При полном отсутствии прав на доступ к объектам компьютерной системы (все элементы соответствующей строки матрицы доступа $a_{ln} = 0$) $\mathcal{A}_{\text{DAC\_Pot}}(u_l, t_k) = 0$.

3. Потенциальная осведомлённость пользователей в конфиденциальной информации в системах мандатного управления доступом

В мандатной модели управления доступом (MAC), как уже отмечалось, права доступа пользователей к объектам определяются по соотношению меток безопасности субъектов и объектов доступа. Метки безопасности conf_i, $i = 1, 2, \ldots, I$ (I — количество уровней конфиденциальности), являются элементами порядковой шкалы абстрактных уровней безопасности. В классической модели мандатного управления доступом множество уровней безопасности рассматривается как линейно упорядоченное множество (линейная решётка). Метки (уровни) безопасности $\text{conf}(u)$, характеризующие пользователей $u \in U$ и соответственно их субъектов $s \in S$, именуются *уровнями доверия*. Метки (уровни) безопасности $\text{conf}(o)$, характеризующие объекты доступа $o \in O$, именуются *уровнями конфиденциальности*.

Права доступа на чтение определяются правилом NRU (No Read Up, «нет чтения вверх»), т. е. пользователь u_l имеет право чтения объекта o_n, если его метка безопасности (уровень доверия) равна или выше метки безопасности объекта (грифа конфиденциальности):

$$\text{conf}(u_l) \geqslant \text{conf}(o_n).$$

Данный порядок определения прав доступа основан на идеологии градуированного доверия пользователям и совершенно не учитывает реальные потребности пользователей в доступе к объектам, исходя из их функциональных обязанностей. Следствием этого является в большинстве случаев избыточность прав доступа, т. е. необусловленность имеющихся прав доступа к объектам с соответствующими грифами конфиденциальности фактическими потребностями конкретных пользователей.

Для устранения избыточности прав доступа, устанавливаемых правилом NRU, в мандатной модели управления доступом дополнительно вводят дискреционную матрицу доступа $\mathbf{A}(t_k)$. Значения матрицы доступа $a_{ln}(t_k)$ определяются, во-первых, правилом NRU, что является необходимым условием:

$$\forall l, n \left(a_{ln}(t_k) \neq \varnothing \Rightarrow \text{conf}(u_l) \geqslant \text{conf}(o_n)\right),$$

а во-вторых, как и в дискреционной модели, фактическими потребностями пользователя u_l в доступе к объекту o_n. В результате при мандатном управлении доступом фактические права доступа пользователей $u \in U$ к объектам $o \in O$ «прописаны» в ячейках той же матрицы доступа $\mathbf{A}(t_k)$.

При этом конфиденциальность объектов является не двоичной величиной (конфиденциально/неконфиденциально, $f_{\text{conf}}(o_n, t_k) \in \{0, 1\}$), а порядковой (порядково-вербальной — $f_{\text{conf}}(o_n, t_k) \in [0, 1]$.

Исходя из этого, потенциальную осведомлённость $\mathcal{A}_{\text{MAC\_Pot}}(u_l, t_k)$ пользователей при мандатном управлении доступом можно определять на основе следующего соотношения:

$$\mathcal{A}_{\text{MAC\_Pot}}(u_l, t_k) = \frac{1}{V(O, t_k)} \sum_{n=1}^{N_{t_k}} a_{ln}(t_k) V(o_n, t_k) f_{\text{conf}}(o_n, t_k),$$

где

$$V(O,t_k)=\sum_{n=1}^{N_{t_k}}V(o_n,t_k)f_{\text{conf}}(o_n,t_k). \tag{3}$$

Отметим, что функция конфиденциальности в выражении (3) отражает не долю конфиденциальной информации в соответствующем объекте, а именно уровень конфиденциальности.

Таким образом, при мандатном управлении доступом уровень потенциальной осведомлённости пользователей в конфиденциальной информации выше не только тогда, когда больше объём доступной пользователю конфиденциальной информации, но и когда выше уровень её конфиденциальности. Иначе говоря, пользователь, который потенциально может владеть большим объёмом конфиденциальной информации невысокого уровня, может оказаться менее осведомлённым (в секретах), чем пользователь, который может потенциально владеть пусть и меньшим объёмом, но существенно более конфиденциальной информацией.

В рамках анализа осведомлённости пользователей в конфиденциальной информации рассмотрим величину $\Delta\mathcal{A}_{\text{MAC\_Pot}}(u_{l_1},u_{l_2},t_k)$:

$$\Delta\mathcal{A}_{\text{MAC\_Pot}}(u_{l_1},u_{l_2},t_k)=|\mathcal{A}_{\text{MAC\_Pot}}(u_{l_1},t_k)-\mathcal{A}_{\text{MAC\_Pot}}(u_{l_2},t_k)|. \tag{4}$$

Лемма 1. Величина (4) неотрицательна, удовлетворяет свойствам симметричности и неравенства треугольника, является частным случаем расстояния Хемминга.

Доказательство. Неотрицательность ($\Delta\mathcal{A}_{\text{MAC\_Pot}}(u_{l_1},u_{l_2},t_k)\geqslant 0$), симметричность ($\Delta\mathcal{A}_{\text{MAC\_Pot}}(u_{l_1},u_{l_2},t_k)=\Delta\mathcal{A}_{\text{MAC\_Pot}}(u_{l_2},u_{l_1},t_k)$) и выполнение неравенства треугольника

$$\Delta\mathcal{A}_{\text{MAC\_Pot}}(u_{l_1},u_{l_2},t_k)\leqslant\Delta\mathcal{A}_{\text{MAC\_Pot}}(u_{l_1},u_{l_3},t_k)+\Delta\mathcal{A}_{\text{MAC\_Pot}}(u_{l_3},u_{l_2},t_k)$$

очевидны по свойствам операции $|a-b|$. Подставляя в соотношение (4) выражения для величин $\mathcal{A}_{\text{MAC\_Pot}}(u_{l_1},t_k)$, $\mathcal{A}_{\text{MAC\_Pot}}(u_{l_2},t_k)$ и производя несложные преобразования, получаем

$$\Delta\mathcal{A}_{\text{MAC\_Pot}}(u_{l_1},u_{l_2},t_k)=\frac{1}{V(O,t_k)}\sum_{n=1}^{N_{t_k}}V(o_n,t_k)f_{\text{conf}}(o_n,t_k)|a_{l_1n}(t_k)-a_{l_2n}(t_k)|.$$

Нетрудно видеть, что сумма в этой формуле является известным расстоянием Хемминга [10] между двоичными векторами прав доступа пользователей u_{l_1} и u_{l_2}, образуемыми соответствующими строками матрицы доступа $\mathbf{A}(t_k)$, координаты которых «взвешены» произведениями параметров $V(o_n,t_k)$ и $f_{\text{conf}}(o_n,t_k)$ объектов доступа. ■

Отметим, что аналогичными свойствами метрики обладает величина $\mathcal{A}_{\text{DAC\_Pot}}(u_l,t_k)$.

Особенности метрики $\mathcal{A}_{\text{MAC\_Pot}}(u_l,t_k)$ иллюстрируются следующим примером.

Пример 1. На рис. 3 приведены расчёты $\mathcal{A}_{\text{MAC\_Pot}}(u_l,t_k)$ для шести объектов доступа с различными параметрами объёма и конфиденциальности информации и информативности объектов и девяти пользователей с различными уровнями доверия в системе с мандатным управлением доступом. Для перевода порядково-вербальных характеристик конфиденциальности в числовые использована следующая эвристика: «высокая степень конфиденциальности» — $f_{\text{conf}}(o_n,t_k)=1$, «средняя» — $f_{\text{conf}}(o_n,t_k)=0{,}809$, «низкая» — $f_{\text{conf}}(o_n,t_k)=0{,}5$.

Рис. 3. Пример потенциальной осведомлённости пользователей при мандатном управлении доступом

Как видно из рис. 3, при наличии прав доступа ко всем объектам, содержащим конфиденциальную информацию, пользователь (на рис. 3 пользователь u_1) характеризуется наивысшей степенью потенциальной осведомлённости 100 %. Заметим, что по правилам мандатного доступа для 100 %-й потенциальной осведомлённости пользователь должен иметь наивысший уровень доверия (на рис. 3 — «высокий»). При этом если с учётом функциональных обязанностей или других соображений пользователь с наивысшим уровнем доверия имеет по матрице доступа права доступа только к некоторым объектам, скажем, только к объектам со степенью конфиденциальности «высокая», то потенциальная осведомлённость такого пользователя может характеризоваться невысокой величиной из-за невысокого объёма информации или информативности соответствующих объектов. Например, пользователь u_2 также с наивысшим уровнем доверия, обладая по матрице доступа правом доступа только к объекту с самым высоким уровнем конфиденциальности (o_3), характеризуется всего лишь 20 %-й величиной потенциальной осведомлённости ввиду незначительного объёма информации соответствующего объекта. Следует, однако, заметить, что данный уровень потенциальной осведомлённости в 20 % является достаточно существенным относительно величины потенциальной осведомлённости пользователей, обладающих правами доступа к другим объектам с существенно большими объёмами информации, но с меньшими уровнями конфиденциальности и информативности.

Чувствительность метрики потенциальной осведомлённости к объёму и уровню конфиденциальности объектов доступа также иллюстрируется показателями $\mathcal{A}_{\text{MAC\_Pot}}(u_l, t_k)$ для пользователей с одинаковым уровнем доверия, но с различными фактическими правами доступа к объектам (по матрице доступа) — пользователи u_3 и u_4, пользователи u_5, u_6, u_7, u_8, u_9.

Анализ поведения метрики $\mathcal{A}_{\text{MAC\_Pot}}(u_l, t_k)$ по приведённым на рис. 3 расчётам позволяет сделать вывод о её соответствии интуитивным представлениям о потенциальной осведомлённости пользователей и, следовательно, о возможности её применения в прикладных системах.

4. Потенциальная осведомлённость пользователей в конфиденциальной информации в системах тематико-иерархического управления доступом

Тематико-иерархическое управление доступом [3, 11, 12] осуществляется на основе сравнения тематических меток (индексов) объектов доступа и тематических меток (полномочий) субъектов доступа (пользователей). В качестве тематических меток объектов и субъектов доступа используются тематические мультирубрики $\mathcal{T}_i^{(m)} = \{\tau_{i_1}, \tau_{i_2}, \ldots, \tau_{i_I}\}$, которые представляют собой наборы рубрик иерархического тематического классификатора $T_{TH} = \{r, \tau_1, \tau_2, \ldots, \tau_K\}$ (иерархического тематического рубрикатора), представляющего собой множество рубрик-тематик $\tau_{i_m} \in T_{TH}$, на котором задано отношение частичного порядка, выражаемое графом вида «корневое дерево» (r — корень дерева) [13]. Самым известным примером такого иерархического тематического рубрикатора является универсальная десятичная классификация (УДК), применяемая в библиотечной сфере для систематизации произведений науки, литературы и искусства, периодической печати, различных видов документов и организации картотек. Мультирубрики $\mathcal{T}_i^{(m)} = \{\tau_{i_1}, \tau_{i_2}, \ldots, \tau_{i_I}\}$ включают наборы элементов τ_{i_m}, которые не находятся между собой в подчинённости по иерархическому рубрикатору, и никакие совокупности (подмножества) элементов мультирубрики не содержат полные совокупности элементов-сыновей каких-либо элементов-отцов иерархического рубрикатора.

Пример 2. На рис. 4 приведён пример корневого дерева иерархического тематического рубрикатора и наборы его рубрик, составляющих мультирубрики. Заметим, что полустепень исхода нелистовых вершин графа не может быть меньше двух, поскольку делить рубрику-тематику на подрубрики-подтематики имеет смысл только тогда, когда число подрубрик не меньше двух.

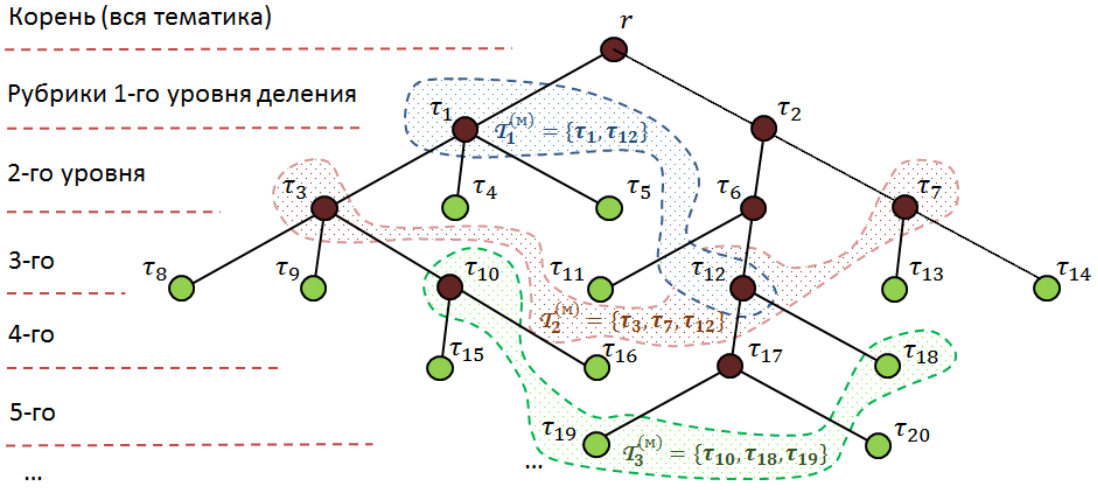

Рис. 4. Пример иерархического тематического рубрикатора и мультирубрик на нём, являющихся тематическими метками объектов доступа и тематическими полномочиями субъектов доступа (пользователей)

Множество мультирубрик $\mathcal{T}_i^{(m)} \in T^{(m)}$ является решёточно-упорядоченным [3, 11, 13] относительно специальной операции доминирования мультирубрик (тематика одной мультирубрики шире тематики другой, т. е. с учётом подчинённости полностью охватывает тематику другой мультирубрики, или мультирубрики несравнимы по отношению «шире — уже», в том числе когда их рубрики-тематики частично пересека-

ются). Если мультирубрика $\mathcal{T}_i^{(m)} = \{\tau_{i_1}, \tau_{i_2}, \ldots, \tau_{i_I}\}$ доминирует над мультирубрикой $\mathcal{T}_j^{(m)} = \{\tau_{j_1}, \tau_{j_2}, \ldots, \tau_{j_J}\}$, то для любой рубрики $\tau_{j_m} \in \mathcal{T}_j^{(m)}$ найдётся рубрика $\tau_{i_n} \in \mathcal{T}_i^{(m)}$, которая совпадает с ней или является старшей по корневому дереву иерархического рубрикатора:

$$\mathcal{T}_i^{(m)} \geqslant T_j^{(m)} \Rightarrow \forall \tau_{j_m} \in \mathcal{T}_j^{(m)} \exists \tau_{i_n} \in \mathcal{T}_i^{(m)} \left(\tau_{i_n} \geqslant_m \tau_{j_m}\right),$$

где $\geqslant_m$ — знак тематического доминирования мультирубрик (тематика шире, т. е. полностью охватывает тематику другой мультирубрики); $\geqslant$ — знак подчинённости или эквивалентности (совпадения) рубрик по корневому дереву иерархического рубрикатора. Таким образом, отношение доминирования мультирубрик как подмножеств рубрик не является отношением теоретико-множественного включения $\subseteq$.

На рис. 4 мультирубрики $\mathcal{T}_1^{(m)} = \{\tau_1, \tau_{12}\}$ и $\mathcal{T}_2^{(m)} = \{\tau_3, \tau_7, \tau_{12}\}$ доминируют над мультирубрикой $\mathcal{T}_3^{(m)} = \{\tau_{10}, \tau_{18}, \tau_{19}\}$: $\mathcal{T}_1^{(m)} \geqslant_m \mathcal{T}_3^{(m)}$, $\mathcal{T}_2^{(m)} \geqslant_m \mathcal{T}_3^{(m)}$, но между собой несравнимы, несмотря на существенное пересечение тематик: $\mathcal{T}_1^{(m)} \geqslant\leqslant_m \mathcal{T}_2^{(m)}$, где знак $\geqslant\leqslant_m$ означает несравнимость мультирубрик.

Как и в мандатных системах, пользователь имеет право чтения объекта по правилу, аналогичному правилу NRU, т. е. когда мультирубрика пользователя (набор разрешённых ему рубрик) доминирует над мультирубрикой объекта доступа.

Аспект возможного изменения состояния системы тематико-иерархического управления доступом будем отображать временно́й зависимостью мультирубрик субъектов и объектов доступа: $\mathcal{T}^{(m)}(u_l, t_k)$, $\mathcal{T}^{(m)}(o_n, t_k)$.

В результате, исходя из положения 4, потенциальная осведомлённость пользователя u_l в момент времени t_k в конфиденциальной информации при тематико-иерархическом управлении доступом $\mathcal{A}_{\text{THA\_Pot}}(u_l, t_k)$ определяется на основе соотношения

$$\mathcal{A}_{\text{THA\_Pot}}(u_l, t_k) = \frac{1}{V(O, t_k)} \sum_{n=1}^{N_{t_k}} V(o_n, t_k)\, \delta(\mathcal{T}^{(m)}(u_l, t_k), \mathcal{T}^{(m)}(o_n, t_k)),$$

где

$$\delta(\mathcal{T}^{(m)}(u_l, t_k), \mathcal{T}^{(m)}(o_n, t_k)) = \begin{cases} 1, & \text{если } \mathcal{T}^{(m)}(u_l, t_k) \geqslant_m \mathcal{T}^{(m)}(o_n, t_k); \\ 0, & \text{если } \left(\mathcal{T}^{(m)}(u_l, t_k) <_m \mathcal{T}^{(m)}(o_n, t_k)\right) \vee \\ & \vee \left(\mathcal{T}^{(m)}(u_l, t_k) \geqslant\leqslant_m \mathcal{T}^{(m)}(o_n, t_k)\right). \end{cases}$$

Нетрудно видеть, что величина $\mathcal{A}_{\text{THA\_Pot}}(u_l, t_k)$ обладает свойствами метрики.

Тематико-иерархическое управление доступом предоставляет дополнительные возможности по анализу потенциальной осведомлённости пользователей в конфиденциальной информации. Поскольку конфиденциальная информация объектов доступа проиндексирована (размечена) тематическими мультирубриками, то появляется возможность анализа осведомлённости пользователей не просто в целом по конфиденциальной информации, обрабатываемой в компьютерной системе, но и по отдельным её тематикам, что может быть важным в тех или иных аспектах информационной безопасности. В частности, по любой простой тематике (одна рубрика-тематика τ_i является частным случаем мультирубрики: $\mathcal{T}_i^{(m)} = \{\tau_i\}$) или по комплексу рубрик-тематик (тематическая мультирубрика $\mathcal{T}_i^{(m)} = \{\tau_{i_1}, \tau_{i_2}, \ldots, \tau_{i_I}\}$) можно определять величину потенциальной осведомлённости $\mathcal{A}_{\text{THA\_Pot}}(u_l, \mathcal{T}_i^{(m)}, t_k)$ пользователя u_l в момент времени t_k:

$$\mathcal{A}_{\text{THA\_Pot}}(u_l, \mathcal{T}_i^{(m)}, t_k) =$$
$$= \frac{1}{V(O, \mathcal{T}_i^{(m)}, t_k)} \sum_{n=1}^{N_{t_k}} V(o_n, t_k)\, \delta\left(\mathcal{T}^{(m)}(u_l, t_k), \mathcal{T}^{(m)}(o_n, t_k)\right) \delta\left(\mathcal{T}^{(m)}(o_n, t_k), \mathcal{T}_i^{(m)}\right),$$

где $V(O, \mathcal{T}_i^{(m)}, t_k)$ — объём всей конфиденциальной информации, тематика которой характеризуется в момент времени t_k мультирубрикой $\mathcal{T}_i^{(m)} = \{\tau_{i_1}, \tau_{i_2}, \ldots, \tau_{i_I}\}$:

$$V(O, \mathcal{T}_i^{(m)}, t_k) = \sum_{n=1}^{N_{t_k}} V(o_n, t_k)\, \delta\left(\mathcal{T}^{(m)}(o_n, t_k), \mathcal{T}_i^{(m)}\right).$$

5. Потенциальная осведомлённость пользователей в конфиденциальной информации в системах ролевого управления доступом

Ролевое управление доступом [14, 15] основывается на понятии роли (точнее — ролевого субъекта доступа) $\rho \in R$ (R — множество ролей), аналогом которой в некомпьютерной сфере является понятие «должность» в организационно-штатной структуре предприятий (организаций) [3]. Пользователи получают права доступа к объектам не напрямую, а посредством разрешения им работы в одной или нескольких ролях. Роли наделяются функционально обоснованной (для соответствующей должности) совокупностью прав доступа к объектам. Функционирование компьютерной системы разбивается на сеансы, работу в которых пользователи начинают с авторизации в одной или нескольких из разрешённых им в системе ролях и осуществляют доступы к объектам по правам соответствующих ролей.

Ролевое управление доступом в системах с большим количеством пользователей и объектов доступа позволяет существенно сократить количество назначений доступа для наделения пользователей необходимыми им для работы правами и в настоящее время широко применяется в корпоративных сетях.

Базовая модель ролевого управления доступом (RBAC, Role Based Access Control), помимо множеств пользователей $u \in U$, объектов доступа $o \in O$ и ролей $\rho \in R$, включает отображение множества U на множество R, наиболее простым и естественным способом задания которого является двоичная $(L \times M)$-матрица W «Пользователи — Роли» (L — количество пользователей, M — количество ролей):

$$W = \begin{array}{c} \\ u_1 \\ u_2 \\ \ldots \\ u_L \end{array} \begin{array}{c} \begin{array}{cccc} \rho_1 & \rho_2 & \ldots & \rho_M \end{array} \\ \begin{pmatrix} 1 & 0 & \ldots & 0 \\ 0 & 1 & \ldots & 1 \\ \ldots & \ldots & \ldots & \ldots \\ 1 & 0 & \ldots & 0 \end{pmatrix} \end{array}. \tag{5}$$

Ненулевые элементы w_{lm} матрицы W означают разрешение работы l-го пользователя в m-й роли.

Права ролевых субъектов доступа часто именуются *полномочиями*, поскольку в расширениях ролевой модели и её практических приложениях включают права запуска (исполнения) определённых функционально-технологических процедур. Упрощённым прототипом таких процедур являются элементарные виды доступа к объектам — «Чтение» (Read), «Запись» (Write), «Выполнение» (Exec).

Наделение ролей полномочиями (в упрощённой трактовке — правами доступа к объектам) может осуществляться на основе одного из двух исходных принципов управления доступом — дискреционного или мандатного (мандатно-ролевые модели) [2, 3], поэтому ролевая модель управления доступом является некой надстройкой над ними. При этом, как отмечалось в п. 3, и при мандатном принципе фактические (итоговые) права конкретных субъектов устанавливаются матрицей доступа, только в данном случае для ролевых субъектов доступа в форме матрицы A_R «Роли — Объекты».

Ввиду рассмотрения доступов только вида «Чтение», матрицу A_R можно считать двоичной, ненулевые элементы $a_{R_{mn}}$ которой отражают разрешение чтения ролевым субъектом ρ_m объекта o_n:

$$A_R = \begin{array}{c} \\ \rho_1 \\ \rho_2 \\ \dots \\ \rho_M \end{array} \begin{array}{c} \begin{array}{cccc} o_1 & o_2 & \dots & o_N \end{array} \\ \begin{pmatrix} 0 & 1 & \dots & 0 \\ 1 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 1 & \dots & 1 \end{pmatrix} \end{array}.$$

С учётом иерархичности отношений в системах организационно-штатной структуры предприятий в наиболее распространённых на практике расширениях базовой ролевой модели на множестве ролей устанавливаются отношения частичного порядка, отображаемые графом типа «корневое дерево».

Пример 3. На рис. 5 приведён пример иерархической организации системы ролей, структура которой представляет граф вида «корневое дерево», полустепень исхода нелистовых вершин в котором может быть равна 1, т. е. старшая роль (должность) может иметь в подчинении всего одну роль (должность).

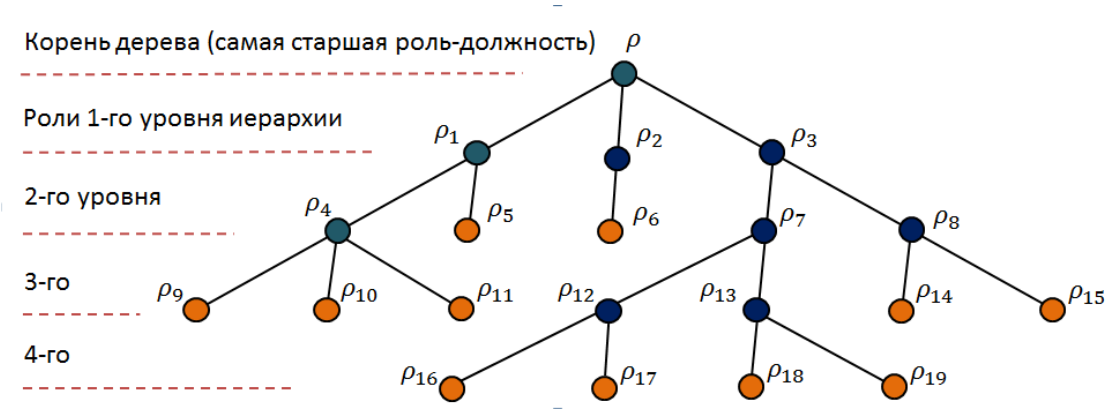

Рис. 5. Пример иерархической системы ролей

Права доступа к объектам и процедурам старших ролей включают права доступа всех подчинённых ролей. Это позволяет ещё больше снизить количество назначений доступа, поскольку полномочия старших ролей могут автоматически складываться только из полномочий подчинённых («листовой» принцип [3]) или из полномочий подчинённых ролей с добавлением их старшим ролям дополнительных («номенклатурных») полномочий (не строго «листовой» иерархически охватный принцип [3]).

Таким образом, в системах с иерархической организацией системы ролей если пользователь в каком-либо сеансе авторизован в определённой роли ρ, то совокупность его

прав доступа охватывает права доступа всех ролей $\rho_i < \rho$, подчинённых по иерархии роли ρ (знак $<$ означает подчинённость по ветви корневого дерева). Определение итоговых прав доступа пользователя в этом случае можно осуществлять на основе матрицы доступа A_R «Роли — Объекты» и матрицы связности (достижимости) $H^{(s)}$ корневого дерева иерархической системы ролей:

$$H^{(s)} = H + H^2 + H^3 + \ldots + H^d,$$

где H — матрица смежности корневого дерева иерархической системы ролей; d — высота дерева, т. е. максимальная длина пути от листовой вершины до корня.

Как и ранее, временно́й аспект функционирования ролевой системы управления доступом будем отображать зависимостью от времени матриц $W(t_k)$, $A_R(t_k)$, $H(t_k)$ и $H^{(s)}(t_k)$.

Ненулевые элементы $h_{ij}^{(s)}(t_k)$ означают подчинённость j-й вершины по иерархии корневого дерева i-й вершине в момент времени t_k — непосредственной (длина пути между вершинами равна 1) либо подчинённости по ветви дерева (длина пути больше 1). Диагональные элементы матриц смежности и связности равны нулю: $h_{ii}(t_k) = 0$, $h_{ii}^{(s)}(t_k) = 0$.

Тогда итоговые права доступа ролей (по непосредственным назначениям и правам доступа подчинённых ролей) задаются элементами матрицы $A_R^{(s)}(t_k)$, которая является произведением матрицы $A_R(t_k)$ на матрицу связности ролей $H^{(s)}(t_k)$, дополненную единичными значениями по диагональным элементам:

$$A_R^{(s)}(t_k) = \left(\left((A_R(t_k))^{\mathrm{T}} \left(H^{(s)}(t_k) + I \right) \right)^{\mathrm{T}} \right)_{|1},$$

где I — единичная матрица; $(x)_{|1} = \begin{cases} 1, & \text{если } x \geqslant 1; \\ 0, & \text{если } x < 1. \end{cases}$

Исходя из этого, итоговые права доступа пользователей в виде матрицы доступа «Пользователи — Объекты» $A_{RW}^{(s)}(t_k)$ в иерархической системе ролей можно определить на основе произведения матрицы $W(t_k)$ на матрицу $A_R^{(s)}(t_k)$:

$$A_{RW}^{(s)}(t_k) = \left(W(t_k)\, A_R^{(s)}(t_k) \right)_{|1}.$$

В результате, исходя из положения 4, потенциальная осведомлённость пользователя u_l в момент времени t_k в конфиденциальной информации при ролевом управлении доступом с иерархически организованной системой ролей $\mathcal{A}_{\mathrm{RBAC\_H\_Pot}}(u_l, t_k)$ определяется на основе следующего соотношения:

$$\mathcal{A}_{\mathrm{RBAC\_H\_Pot}}(u_l, t_k) = \frac{1}{V(O, t_k)} \sum_{n=1}^{N_{t_k}} V(o_n, t_k)\, a_{RW}^{(s)}(t_k).$$

Нетрудно показать, что величина $A_{\mathrm{RBAC\_H\_Pot}}(u_l, t_k)$, как и аналогичные величины при дискреционном, мандатном и тематико-иерархическом управлении доступом, удовлетворяет требованиям метрики.

Заключение

Использование метрик $\mathcal{A}_{\text{DAC\_Pot}}(u_l, t_k)$, $\mathcal{A}_{\text{MAC\_Pot}}(u_l, t_k)$, $\mathcal{A}_{\text{THA\_Pot}}(u_l, t_k)$ и $\mathcal{A}_{\text{RBAC\_H\_Pot}}(u_l, t_k)$ может являться основой специального программного инструментария не только для анализа состояния существующей (функционирующей) системы прав доступа пользователей, но и средством проектирования системы управления доступом пользователей к конфиденциальной информации. Администраторы компьютерных систем, выстраивая систему прав доступа или анализируя её текущее состояние, могут видеть значения и тенденции в потенциальной осведомлённости тех или иных пользователей и принимать на этой основе решения в контексте обеспечения информационной безопасности.

Параметры объёма информации объектов доступа $Q(o_n, t_k)$ в словах, как правило, автоматически определяются и включаются в метаданные текстовых файлов в современных офисных системах работы с документами и системах электронного документооборота.

Порядково-вербальные характеристики конфиденциальности информации $f_{\text{conf}}(o_n, t_k)$ в мандатных системах управления доступом устанавливаются на основе процедур, закрепляемых нормативными регламентациями делопроизводства, и также, как правило, включаются в метаданные файлов офисных систем и систем электронного документооборота. Подобные же по смыслу и содержанию процедуры могут быть регламентированы для определения характеристик информативности объектов доступа $\theta(o_n, t_k)$. К примеру, уровень информативности документа устанавливает его исполнитель и/или выделенный сотрудник (аналитик).

Отдельно следует отметить проблемы построения (обоснования) эвристик перевода (отображения) порядково-вербальных характеристик конфиденциальности в числовую шкалу $[0, 1]$ в системах с мандатным управлением доступа.

Насколько известно, строгих и корректных процедур такого рода преобразований не существует. Объективной причиной этого является различная информативность порядковых и количественных шкал. Показания количественной шкалы $[0, 1]$ помимо порядка отображают (воспроизводят) расстояния между оцениваемыми объектами по соответствующим характеристикам. Таким образом, переводя оценки из порядковой шкалы в количественную, необходимо сформировать дополнительную информацию о расстояниях по соответствующему свойству/показателю между оцениваемыми объектами.

Обратные преобразования (из числовой шкалы $[0, 1]$ в порядковую) осуществляют на основе интервального принципа, разбивая диапазон $[0, 1]$ на равные или неравные интервалы, все числовые элементы из которых объединяются в соответствующие отсчёты (показатели) порядковой шкалы. При этом происходит потеря информации о расстояниях и применяются опять-таки определённые эвристики. Наиболее часто такие эвристики основываются на гипотезе о равных интервалах, согласно которой диапазон шкалы $[0, 1]$ разбивается на одинаковые по величине интервалы, каждый из которых соответствует своему отсчёту на шкале порядка.

Другим принципом разбиения шкалы $[0, 1]$ на порядковые интервалы может быть принцип «золотого сечения» («золотой пропорции»), согласно которому меньшая часть целого (следующий, более высокий отсчёт порядка и соответствующий интервал) относится к большей части целого (первый отсчёт порядка) так же, как большая часть относится к целому. Тогда двум отсчётам в порядковой шкале «низкий — высокий» соответствуют два интервала на шкале $[0, 1]$ — (0, 0,618) и (0,618, 1). Одним из вариантов разбиения шкалы $[0, 1]$ на три порядковых интервала по принципу «золотой

пропорции» может быть разбиение «верхнего» интервала (0,618, 1) также по принципу «золотой пропорции». В результате диапазон шкалы $[0, 1]$ разбивается на три интервала — низкий (0, 0,618), средний (0,618, 0,854) и высокий (0,854, 1). Другим вариантом разбиения диапазона шкалы $[0, 1]$ на три порядковых интервала может быть добавление к отрезку $[0, 1]$ третьего отрезка, который соотносится с меньшим интервалом двухуровневого разбиения, т. е. с интервалом (0,618, 1), по принципу «золотой пропорции». Длина такого отрезка равна 0,235999937. Нормируя увеличенный диапазон шкалы (0, 1,235999937) на единичную длину, получаем следующие три интервала — низкий (0, 0,499994), средний (0,499994, 0,809), высокий (0,809, 1).

Исходя из интервального принципа, эвристики преобразования показателей из порядково-вербальных шкал в шкалу $[0, 1]$ заключаются в присвоении всем объектам оценки, характеризующимся определённым показателем шкалы порядка, такого числового значения на шкале $[0, 1]$, которое соответствует определённой характеристике соответствующего интервала (обычно левой/правой границе или середине интервала). Соответственно различия в конфиденциальности в шкале $[0, 1]$ тех или иных объектов доступа внутри интервалов нивелируются.

Таким образом, программно-техническая составляющая систем анализа потенциальной осведомлённости пользователей на основе представленных метрик с учётом отмеченных эвристик может быть реализована в современных офисных системах работы с документами и системах электронного документооборота.

ЛИТЕРАТУРА

1. *Ушаков Д. Н.* Большой толковый словарь русского языка. М.: Дом Славянской кн., 2008. 959 с.
2. *Девянин П. Д.* Модели безопасности компьютерных систем. Управление доступом и информационными потоками. М.: Горячая линия-Телеком, 2020. 352 с.
3. *Гайдамакин Н. А.* Разграничение доступа к информации в компьютерных системах. Екатеринбург: Изд-во Урал. ун-та, 2003. 328 с.
4. *Грушо А. А., Применко Е. А., Тимонина Е. Е.* Теоретические основы компьютерной безопасности. М.: Издательский центр «Академия», 2009. 272 с.
5. *Shannon C. E.* A mathematical theory of communication // Bell System Technical J. 1948. V. 27. P. 379–423.
6. Р 50.1.053-2005. Информационные технологии. Основные термины и определения в области технической защиты информации. М.: Стандартинформ, 2005. 11 с.
7. ГОСТ Р ИСО/МЭК 27000-2021. Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология. М.: Стандартинформ, 2021. 21 с.
8. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ (с изм.). Собрание законодательства Российской Федерации. 2006. № 31. Ст. 3448.
9. ГОСТ Р 58545-2019. Менеджмент знаний. Руководящие указания по сбору, классификации, маркировке и обработке информации. М.: Стандартинформ, 2019. 34 с.
10. *Деза Е. И., Деза М. М.* Энциклопедический словарь расстояний. М.: Наука, 2008. 446 с.
11. *Гайдамакин Н. А.* Модель тематического разграничения доступа к информации при иерархической структуре классификатора в автоматизированных системах управления // Автоматика и телемеханика. 2003. № 3. С. 177–189.
12. *Гайдамакин Н. А.* Многоуровневое тематико-иерархическое управление доступом (MLTHS-система) // Прикладная дискретная математика. 2018. № 39. С. 42–57.

13. *Гайдамакин Н. А., Баранский В. А.* Алгебра мультирубрик на корневых деревьях иерархических тематических классификаторов // Сиб. электрон. матем. изв. 2017. Т. 14. С. 1030–1040.
14. *Ferrariolo D. F. and Kuhn D. R.* Role Based Access Control // 15th National Computer Secure Conf. Baltimore, 1992. P. 554–563.
15. *Sundhu R., Coyne E. J., Feinstein H. L., and Youman C. E.* Role-Based Access Control models // IEEE Computer. 1996. V. 29. No. 2. P. 38–47.

REFERENCES

1. *Ushakov D. N.* Bol'shoy tolkovyy slovar' russkogo yazyka [Great Dictionary of Russian Language]. Moscow, Dom Slavyanskoy kn., 2008. 959 p. (in Russian)
2. *Devyanin P. D.* Modeli bezopasnosti komp'yuternykh sistem. Upravlenie dostupom i informatsionnymi potokami [Security Models of Computer Systems. Access and Information Flow Management]. Moscow, Goryachaya liniya-Telekom, 2020. 352 p. (in Russian)
3. *Gaydamakin N. A.* Razgranichenie dostupa k informatsii v komp'yuternykh sistemakh [Differentiation of Access to Information in Computer Systems]. Ekaterinburg, UrFU Publ., 2003. 328 p. (in Russian)
4. *Grusho A. A., Primenko E. A., and Timonina E. E.* Teoreticheskie osnovy komp'yuternoy bezopasnosti. [Theoretical Foundations of Computer Security]. Moscow, Publishing Center "Akademiya", 2009. 272 p. (in Russian)
5. *Shannon C. E.* A mathematical theory of communication. Bell System Technical J., 1948, vol. 27, pp. 379–423.
6. R 50.1.053-2005. Informatsionnye tekhnologii. Osnovnye terminy i opredeleniya v oblasti tekhnicheskoy zashchity informatsii [R 50.1.053-2005. Information Technology. Basic Terms and Definitions in the Field of Technical Information Protection]. Moscow, Standartinform Publ., 2005. 11 p. (in Russian)
7. GOST R ISO/MEK 27000-2021. Informatsionnye tekhnologii. Metody i sredstva obespecheniya bezopasnosti. Sistemy menedzhmenta informatsionnoy bezopasnosti. Obshchiy obzor i terminologiya [GOST R ISO/IEC 27000-2021. Information Technology. Methods and Means of Ensuring Security. Information Security Management Systems. General Overview and Terminology]. Moscow, Standartinform Publ., 2021. 24 p. (in Russian)
8. Federal'nyy zakon "Ob informatsii, informatsionnykh tekhnologiyakh i o zashchite informatsii" [Federal Law "On information, information technologies and on information protection"]. 27.07.2006, no. 149-FZ. Collection of Legislation of the Russian Federation, Moscow, 2006, no. 31, st. 3448. (in Russian)
9. GOST R 58545-2019. Menedzhment znaniy. Rukovodyashchie ukazaniya po sboru, klassifikatsii, markirovke i obrabotke informatsii [GOST R 58545-2019. Knowledge management. Guidelines for the collection, classification, labeling and processing of information]. Moscow, Standartinform Publ., 2019. 34 p. (in Russian)
10. *Deza E. I. and Deza M. M.* Entsiklopedicheskiy slovar' rasstoyaniy [Encyclopedic Dictionary of Distances]. Moscow, Nauka, 2008. 446 p. (in Russian)
11. *Gaydamakin N. A.* A model of thematic differentiation of access to information for the hierarchical classifier in automatic control systems. Autom. Remote Control, 2003, vol. 64, no. 3, pp. 505–516.
12. *Gaydamakin N. A.* Mnogourovnevoe tematiko-ierarkhicheskoe upravlenie dostupom (MLTHS-sistema) [Multilevel thematic-hierarchical access control (MLTHS-system)]. Prikladnaya Diskretnaya Matematika, 2018, no. 39, pp. 42–57. (in Russian)
13. *Gaydamakin N. A., Baranskiy V. A.* Algebra multirubrik na kornevykh derevyakh iyerarkhicheskikh tematicheskikh klassifikatorov [Algebra of multirubric on root trees

of hierarchical thematic classifiers]. Sib. Èlektron. Mat. Izv., 2017, vol. 14, pp. 1030–1040. (in Russian)

14. *Ferrariolo D. F. and Kuhn D. R.* Role Based Access Control. 15th National Computer Secure Conf., Baltimore, 1992, pp. 554–563.
15. *Sundhu R., Coyne E. J., Feinstein H. L., and Youman C. E.* Role-Based Access Control models. IEEE Computer, 1996, vol. 29, no. 2, pp. 38–47.